VOLUME IV
FLIGHT TEST MANAGEMENT

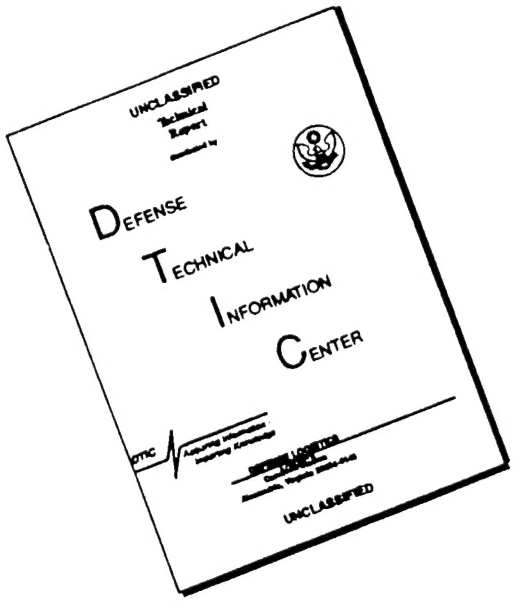
CHAPTER 3

SYSTEMS / TEST SAFETY

DECEMBER 1990

USAF TEST PILOT SCHOOL
EDWARDS AFB, CA

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

SYSTEMS SAFETY

Systems Safety has been called a number of things over the years. It has been called Design Safety; it's been called Engineering Safety, Planning or Management Safety. Systems Safety encompasses all of those. A system is considered as all the equipment, all the actions, all the parts necessary for operation. For example, the F-16 system does not just refer to X number of airplanes and pilots, but the whole system; with crew training, the syllabus of instruction for all the maintenance personnel, the software tapes that go into producing the automatic test equipment, the Seek Eagle or Stores Qualification program conducted here at the Center to qualify and determine the delivery procedures for all the external stores and weapons carried on the airplane, etc.

Now consider for a moment your role as a test engineer and a test pilot and the overall design in testing of an airplane or a weapon system. You are the last person in the design effort to review the safety of that machine or device before it's produced and delivered to your compatriots out in the field. It's up to you to identify the faults and hazards of those systems and get them corrected before they are turned loose to the operational field.

Consider for a moment some of the equipment that you've been flying around the Air Force over the past years and the hazard associated with those systems. Maybe you've wondered why those problems exist, and why they weren't discovered and corrected while the airplane was being tested. For

(3.2,3.3 Deleted)

example, those of you who have flown the F-4 will recall that when you put your gear down, more often than not, you'll lose your TACAN. It's a design fault in the airplane and particularly the location of the TACAN antenna on the nosegear door. When the wheels are down, the gear doors turn 90 degrees and now the antenna is parallel to the fuselage of the airplane frequently causing the TACAN to break lock. Is that design fault an oversight on the part of the test pilot and the test engineers who conduct the original development test on the F-4? The answer is "no". Read the final technical report on the F-4 series of aircraft; you will find the conclusion that the TACAN breaks lock, with the gear down and the recommendation that this be fixed. It was never done and you might ask why. Characteristically, the reports that you spend so much time and effort preparing are never read by the Program Manager, or at least not in time to act upon your recommendations. However, there are two tools at our disposal, through the Systems Safety process, that will assist you in correcting these kinds of design faults. First, in the overall systems safety process; the SPO or the Program Manager forces the contractor to design safety into his system, to review any faults or any hazards discovered during the testing and to sit down with you, the tester, the program manager, the user, or and the logistics command to discuss these problems periodically. Therefore problems like this are recognized at the time that they occur, rather than some time later when the final report is prepared. One other tool to promote identification of design faults, is a new Section V of Tech Order 00-35D-54. This tech order deals with what is known as service reports, previously called deficiency reports. (See Attachment 1 for details.) As

testor you cite the deficiency shortly after discovery and identify it to the program manager, who may close it out without action or may put up the money and give direction to the contractor to correct the problem. This is a very powerful tool for correcting flaws similar to the F-4 TACAN example. Recently in that a new flight director was to be incorporated on the airplane. The flight director had a series of faults, some of which were downright hazardous. Because of service reports and prompt reaction by the SPO to systems safety working group discussions, fixes were developed and implemented prior to the final test report submission. The report, having been in typing for so long, concluded that the flight director did not work correctly and recommended that it be fixed. By prompt action by the test pilot and test engineer, this design fault was corrected before the final report was ever published!

It's important to understand the role of safety in management. Too often you think of the role of a safety staff as being a cop who goes out and arrests someone for being unsafe. That may be the case in certain types of operations, but this is not the case in system safety. To change designs or operations costs time and money. Changes are very expensive. For example, it costs $25,000 to put a simple decal on a fleet of F-4 aircraft. Complicated design hardware changes, of course, will be much more costly. In order to change the design of the system, you must have legitimate claims, backed up by clear logic which can convince the program manager that any changes are warranted. He is concerned with cost, schedule, and performance. If you can show where the added safety will improve the performance of the system to a point where it is cost beneficial to do so,

then you have a good chance to convince him. Without that kind of logic, you will not get the changes that you recommend. These notes will expose you to some of the logic by which you can measure performance and justify changes to hazardous operations or designs.

The systems safety process is a requirement levied upon all services by Department of Defense Instruction 5000.36. That DODI is implemented in the Air Force by AFR 800-16. It is implemented in Systems Command through AFSC AFFTC supplements to AFR 127-2. All the Services have adopted Mil Standard 882.B, which defines the systems safety process to be implemented by contractors when developing and designing new systems. There are two other additional source documents dealing with systems safety: Systems Command Design Handbook 1-6, and our local Air Force Flight Test Center Regulation 127-3. All implement systems safety process on us here at Edwards AFB.

The Program Manager, or the SPO, buys a system safety program from the contractor similar to going to the supermarket and buying a can of beans. Basically these regulations direct us to buy that can of beans, the system safety process. The program manager has four different program levels of system safety that he can buy. A document called a data item description (DID) describes this "can of beans" that you buy from the contractor. You order that data on a particular form called a DD Form 1664. That product then becomes a part of the contractor data requirements list (CDRL). There are four DID dealing with system safety (see Attachment III). First of all is DI-H-7047, which is the Systems Safety Program Plan. This DID describes who is doing what, to whom, and when they are to do it. The next DID is a

DI-H-7048, Systems Safety Hazard Analysis Report which defines the type of analyses the contractor will perform and when these will be delivered. These two products are generally required for major test programs, say for example the design of an F-19, or F-20, or B-3, should those come to pass. For lesser programs, you can buy a smaller can of beans. DI-H-7049, the Safety Assessment Report, is often used for small development programs, and finally, DI-H-7050, System Safety Engineering Report, is used for periodic reviews or for minor changes like ECPs, Class II modifications, etc.

When designing systems, there is an obvious system safety precedence. First you should design to eliminate hazards entirely and make the system Murphy-proof. Obviously this cannot always be done, so your next choice is to provide safety devices to minimize the hazard. For example, relief valves on pressure tanks or protective devices such as clothing worn by individuals working with caustic material. If the problem cannot be eliminated or a suitable safety device cannot be designed, then you should provide warning devices. You are familiar with the fire detection systems, pedal shakers, warning horns, etc., installed on aircraft. And finally, the last of the safety priorities is a procedures change. A change can be minimized by the introduction of a Note, a Warning or Caution in the Flight Manual. All too often this is taken as the easy way out. Notes and changes in Flight Manuals come cheap, and it is very tempting to use these as the corrective action for a major design fault. But what help is it to the F-4 pilot to put a note in the flight manual saying "WARNING, YOU MAY LOSE YOUR TACAN WHEN YOU PUT YOUR GEAR DOWN." That doesn't do him much good when he's in the soup, groping from the final approach fix to the touchdown point

without a GCA. Obviously precedence depends on how much money you have and how severe the hazard is. That is the heart of the system safety process: defining hazards, defining risk and calculating what to pay for corrections. The whole overall system safety process is somewhat analogous to forecasting the future: trying to identify hazards, and trying to eliminate them from the system.

The use of Lessons Learned to understand the mishaps and mistakes of the past are invaluable in predicting what will happen in the future. Historical data, available to you as the design engineer, the test engineer, or the test pilot on a particular program, include the following:

a. First of all is the Air Force AFSC Design Handbook series which has a good catalog of designs and lists of various standards, codes and specifications for various systems, not only aircraft, but physical plants as well.

b. The military, government, or professional codes and standards. For example the electricity in buildings is covered by electrical codes, fire protection codes, etc. These are very important to the design engineer to minimize the potential for mishap or to reduce the nature of any catastrophe, in case one does occur.

c. There are also comprehensive programs in lessons learned throughout the Air Force. Air Force Systems Command Regulation 800-10 obliges each of the major test centers to prepare a lessons learned annually. These documents are available at the library and lessons can be applied when

planning and conducting flight test programs.

d. In addition, Air Force Acquisition Logistics Division, a major division of AFLC, has a retrieval system through which lessons learned can be derived from field reports sent by the various users, Air Logistics Centers, and item and system managers throughout the AFLC system.

e. Don't forget the Air Force Inspection and Safety Center at Norton which has a huge data base on all sorts of mishaps and causes. This information is available to you as a test program manager and designer. All that is required is to call to Norton and they will be glad to oblige and will assist you by providing existing data or by even designing a separate data tailored to your needs.

f. Throughout the Center there are all sorts of reports on past programs. These reports tell not only how the program was structured, and how it was conducted, but in all the reports since 1978 the safety planning data is also included. Safety planning data not in these test reports is available in the System Safety Office or the Tech Library. These data are known as the AF System Command Form 5028 and deals with the safety and test planning to conduct the test. At the end of each test program a final closeout memo for record is prepared discussing the adequacy of safety planning. "Was it too restrictive; did it overlook hazards that occurred or were there any unusual occurrences." These forms are on file at the System Safety Office and information such as, test type, aircraft type, key test words, and test process changes are maintained on a computer data base for easy access by all project personnel.

g. Talk to the old heads. There are numerous folks at the Center and throughout Systems Command who have conducted tests for years on a number of

systems. The use of that corporate memory is invaluable in conducting test programs.

The primary thrust of the system safety process is to determine the hazards associated with the particular design, plan, or concept, and to make value judgments as to the acceptability of the risk involved. These processes are known as hazard analysis and risk management respectively. There are three generally accepted schemes of determining and evaluating hazards: the first involves inductive logic, often referred to as "from the bottom to the top," which generates a specific situation to an overall effect. Secondly, deductive logic, "from the top down," reasons from a general result down to the specific cause; and finally, intuitive logic is another way of saying "experience."

Let's begin with inductive type logic, "bottom to the top type analysis." Consider the electrical system on your automobile. Look at the specific fault modes in the voltage regulator. If the points in your regulator freeze closed, what would be the overall effect on your car's operation? Obviously if they are frozen closed the output current from the alternator will be excessive and will eventually boil your battery dry or even cause it to explode. Eventually you will be unable to make future starts although you can probably continue to run for quite some time with the points frozen together. On the other hand, if the points were stuck apart so no excitation current is provided to your alternator, and there would be no output and the battery would eventually discharge. The distance you could travel would be dependent on the rate of electrical drain on the

battery but eventually the automobile will no longer run. Such analysis is called "failure mode and effective analysis." Starting with the bottom, specific "black box" or some of the simple parts of that black box, failures are generalized effect to the overall system. This is "bottom to the top" or inductive type reasoning.

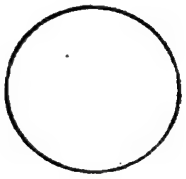
Now consider the top down or deductive type reasoning. The general event is car failure to run. Why would your car cease to run? It could be stopped for a number of reasons but let's start very simply. For example, if your car will not start in the morning, it could be one of two common reasons. One - you don't have sufficient fuel to the engine, or secondly, you don't have the proper ignition. There are several ways you may not have proper fuel: you may be out of fuel; maybe the fuel mixture is too rich; or maybe the fuel mixture is too lean. On the other hand, why would you not have spark? Maybe there is a complete absence of spark. Maybe the spark is too weak or maybe the spark is occurring at the wrong time. You could further analyze why each of those events did not occur and would finally arrive at some probable causes through logic from the top down. That particular type of logic is most commonly used in system safety hazard analysis and the particular method in which it is used is called fault tree analysis.

Fault tree logic uses a convention which is shown in figure 1.

SYMBOLS

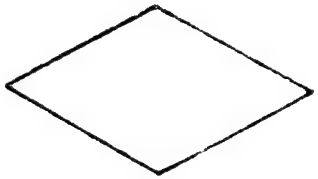
EVENTS

THE HOUSE INDICATES AN EVENT THAT IS NORMAL



THE CIRCLE IDENTIFIES A BASIC FAILURE

THE RECTANGLE IDENTIFIES AN EVENT THAT RESULTS FROM A COMBINATION OF FAULT EVENTS

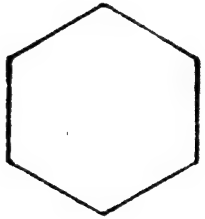


THE DIAMOND IDENTIFIES A FAILURE THAT HAS NOT BEEN FULLY DEVELOPED BECAUSE OF LACK OF INFORMATION OR SIGNIFICANCE

OPERATORS

THE "AND" GATE DESCRIBES THE LOGICAL OPERATION THAT REQUIRES THE COEXISTENCE OF MORE THAN ONE INPUT TO CAUSE THE OUTPUT

THE "OR" GATE DESCRIBES THE LOGICAL OPERATION WHEREBY THE OUTPUT IS CAUSED BY THE OCCURRENCE OF ANY OF THE INPUTS



THE INHIBIT GATE INDICATES A RESTRICTION TO SEQUENCE WHICH REQUIRES AN INPUT AND RESTRICTION TO OCCUR FOR AN OUTPUT TO BE GENERATED

THE TRANSFER SYMBOL IS USED TO SHOW CONTINUITY BETWEEN TWO PARTS OF THE TREE. A LINE INTO THE SIDE OF THE TRIANGLE TRANSFERS EVERYTHING BELOW TO ANOTHER AREA IDENTIFIED BY THE TRIANGLE WITH A LINE DRAWN FROM THE APEX.

FIGURE 1

Consider the simple system shown in figure two. It is a typical air compression that you might find in a filling station; an electrical motor powers an air pump. When the air reaches sufficient pressure a pressure-activated switch shuts off electrical power, terminating pump operation. Consider a hazard of the tank exploding: a simple fault tree analysis would look as shown in figure three.

What importance is this to you as the design engineer or the test manager? A fully developed fault tree may cover enough space to paper a whole wall the size of the classroom in the Test Pilot School.

Consider the simple analysis shown in figure four. An undesired event could occur as a result of a combination of any four different events - a, b, c, or d. The probability, shown to the side of the"a," "b," "c," or "d" is the likelihood that those would occur. If you were the design engineer and had a limited budget to reduce the probability of occurrences of any of those four events, to which would you apply your money? At first glance it would seem most obvious that you should reduce "d" since that is by far the most likely of the events to occur. However, if you consider the fault tree you will see that the overall undesired event will occur anytime "a" happens by itself. That is called a single point failure. The probability of the overall undesired event is .005, the same as "a." Only one other unique combination of events will cause the overall undesired event: "b" and "c" and "d" all occurring simultaneously. The probability that all three occur simultaneously is "a" x "b" x "c" or .000006, a very unlikely event. Of course, you see that "b" and "a" could cause the event or "a" and "b" and

A SIMPLE SYSTEM

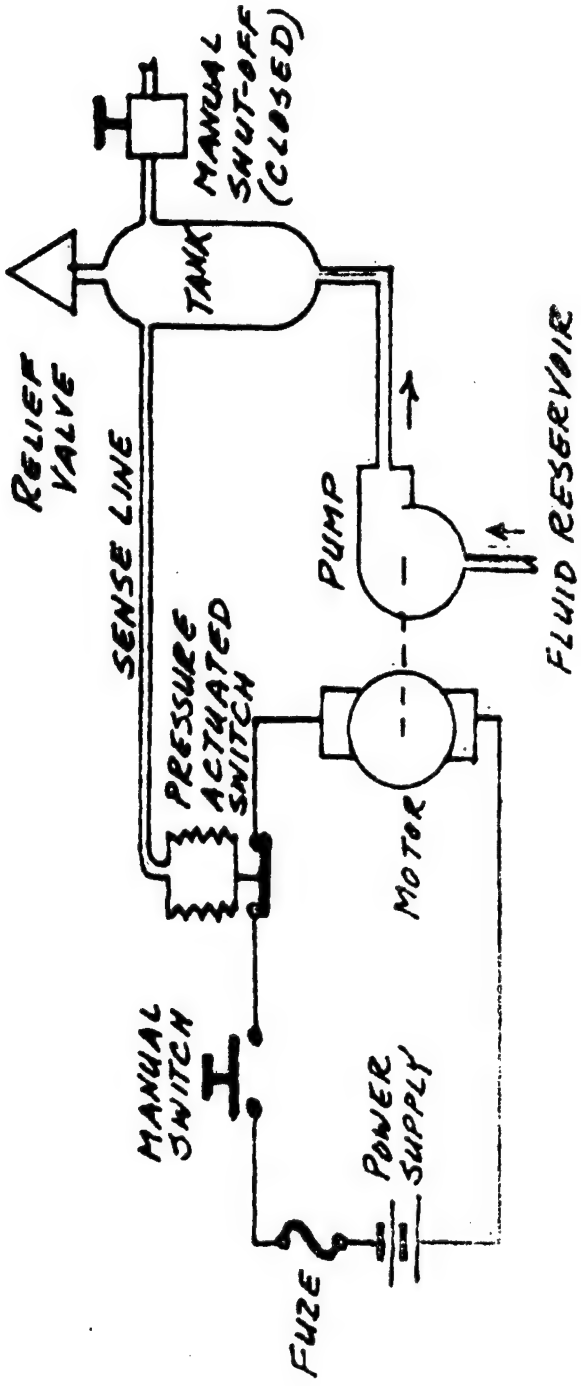


FIGURE 2

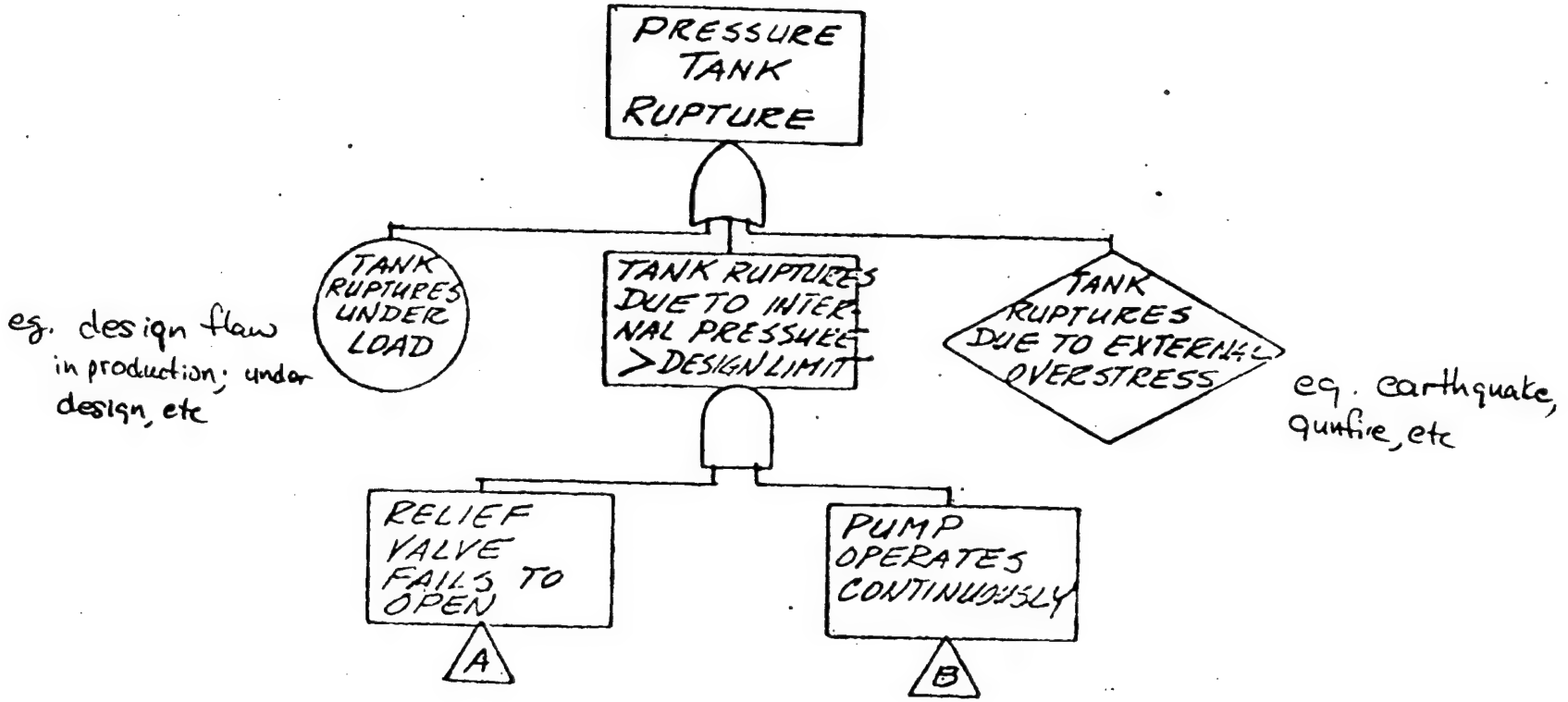

PRESSURE TANK RUPTURE
TANK RUPTURES UNDER LOAD
TANK RUPTURES DUE TO INTERNAL PRESSURE > DESIGN LIMIT
TANK RUPTURES DUE TO EXTERNAL OVERSTRESS
RELIEF VALVE FAILS TO OPEN
PUMP OPERATES CONTINUOUSLY
A
B
eg. design flaw in production, under design, etc
eg. earthquake, gunfire, etc

FIGURE 3

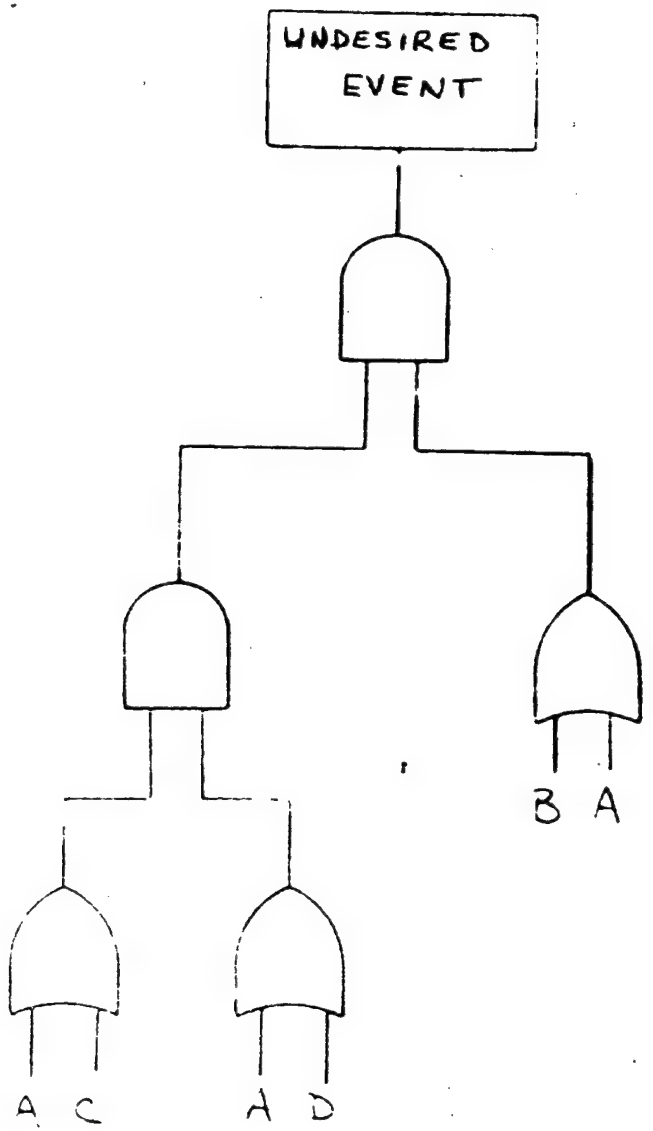


FIGURE 4

A = .005
B = .01
C = .02
D = .03

A = .005
* B+A = (.005)(.01)
* A+D+C = (.005)(.03)(.02)
B+C+D = (.01)(.02)(.03) =
.000006

* trivial solutions

"c" could occur - these are however trivial since "a" will have triggered the event already. Very complicated systems can be analyzed quickly, by computer processes now available to safety design engineers, to identify single point failures, dual point failures, and three point failures, etc., on very complex systems fault tree analysis can identify where the hazards are most likely to occur.

Intuitive logic, or experience, can be brought to use in a variety of manners. One way is the use of the hazard analysis similar to that we use in the AF Systems Command Form 5028; there are many other variants of this sort of document throughout industry and some are shown in figures 5-7 . Generally they follow the format: hazard, cause, effect, hazard category (in terms of MILSPEC, 882B), and finally, corrective action that will minimize or reduce these hazards.

Another very powerful technique in identifying unique hazards is called a sneak circuit analysis. Consider figure 8. This is a portion of the typical electrical system in an automobile. The radio is normally played by turning on the ignition switch and the radio. Note that with the ignition switch on and pressing on the brake pedal lights up the tail lights. The emergency flasher switch also lights up the tail lights. Now, consider this: Your ignition switch is off. (Normally you would not be able to operate the radio.) You turn on the emergency flasher and press on the brake pedal. Power would now be applied to operate the radio intermittently! That is known as a sneak circuit. While of some casual interest here, it is no hazard. However, if this were not a radio but a

(3.18-3.20 Deleted,
figures 5,6,7 Deleted)

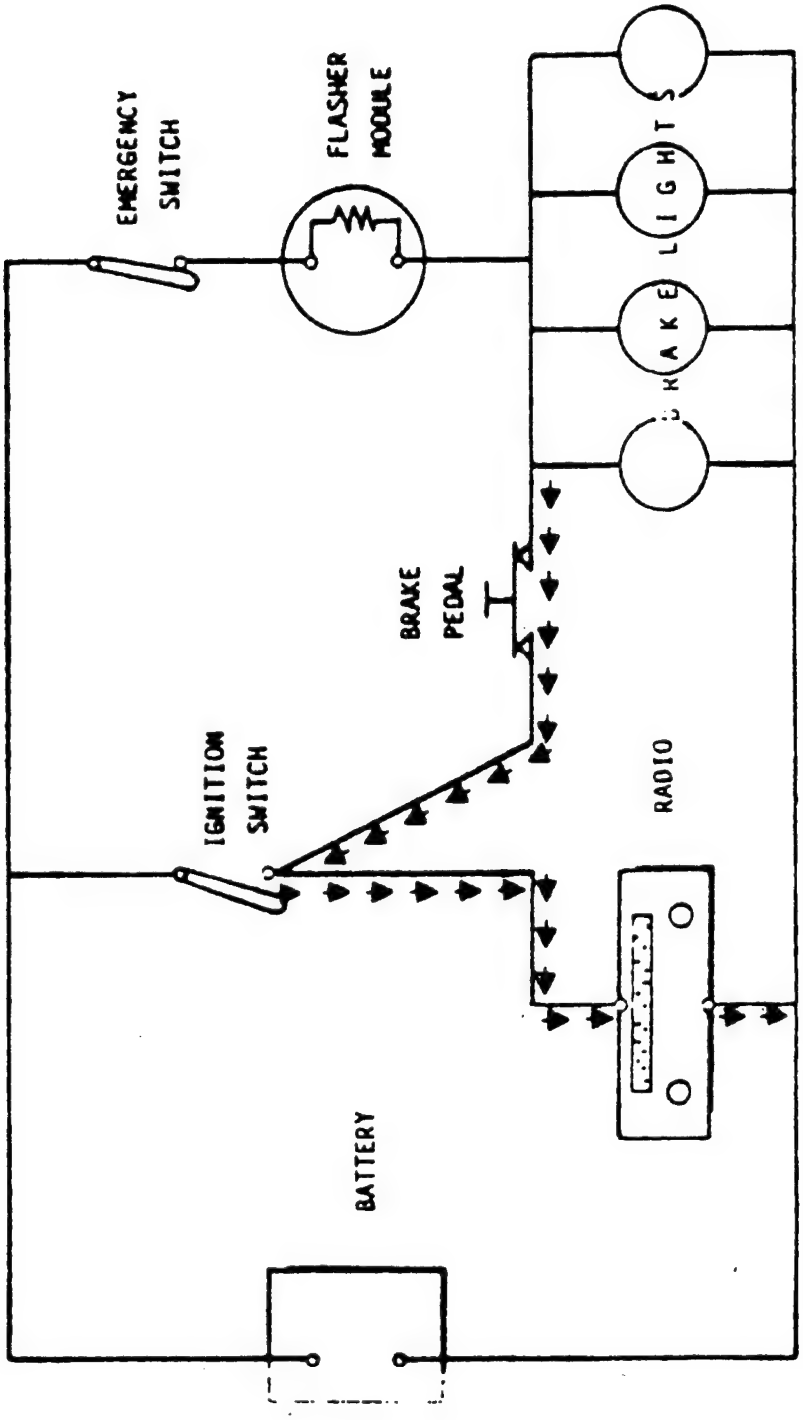

EMERGENCY SWITCH
FLASHER MODULE
BRAKE LIGHTS
BRAKE PEDAL
IGNITION SWITCH
RADIO
BATTERY

FIGURE 8

pyrotechnic device, the result of a sneak circuit could be catastrophic.

Sneak circuits can sometimes be of value. NASA discovered that an experiment in a spacecraft could be initiated through a sneak circuit. NASA considered it not to be a safety hazard and the wiring remained unchanged. When the space craft was in orbit this particular experiment did not function when the switch was turned on. NASA was able to operate the experiment through the use of the sneak circuit.

Let us examine risk assessment. The risk is nothing more than the product of the severity of a mishap, should it occur, and the frequency, in which it will occur, or alternately, is severity, the rate and the exposure factor: R = Sxf = SxRxt.

Consider for a moment this sample: If someone were to borrow my pickup truck, I could evaluate the risk in actual terms. The cost of the pickup from the Red Book, might be $5,000. To determine the accident rate I look at Air Force accident records for the past several years to find that the accident rate is approximately three accidents per million miles. My neighbor wanted to borrow the vehicle to drive 200 miles; the risk, to me, would be shown by the following equation: 3.00 = $5,000 x 3/1,000,000 x 200 the risk it involves about $3.00 or a cent and a half per mile, assuming I have no comprehensive insurance. That would be a method of evaluating an insurance policy, if I can buy insurance for less than a cent and a half per mile it would be in my benefit to buy that insurance. If it were more than that, then I would consider self-insuring. Safety devices and system safety planning can be considered similarly. Unfortunately, in the real world

predicting actual rates and actual exposures is not precise. Exact physical probabilities are usually anavailable and you must rely on subjective type analysis. Three subjective type analysis will be presented.

First of these methods is known as the Risk Assessment Code (RAC). Consider figure 9. The hazard levels, defined by severity, are broken into four broad categories ranging from catastrophic to negligible. (These Categories I, II, III, and IV, are defined in MIL STANDARD 882 B.) The likelihood the hazard will occur is identified alphabetically "a" through "d." Something likely to occur within a short period of time is assigned probability "a," something unlikely as to occur is assigned probability "d." The severity and likelihood levels are combined into a matrix as shown in figure 9c. This method is often used when a hazard is identified on a hazard report submitted to the Flight Test Center. The Arabic numbers in the matrix 1 through 6 assist the manager or the commander in prioritizing use of his limited funds or personnel to correct hazards that are reported to him. He will start with the lowest numbers and apply his time and energy to solving those, leaving the 5s and 6s to be fixed last.

In our system safety planning at the Flight Test Center we use a procedure similar to the risk assessment code. Using the same hazard categories as defined by MIL STANDARD 882 B, we define three levels of hazard probabilities: high, medium or low (see figure 10). The slanted lines define three levels of risk: The upper left hand corner equates to Hazardous Tests. (Category I or II and high probability of occurrence. During a hazardous test the Center Commander must be briefed prior to each

HAZARD LEVELS

CATEGORY I: CATASTROPHIC - MAY CAUSE DEATH OR SYSTEM LOSS.

CATEGORY II: CRITICAL - MAY CAUSE SEVERE INJURY, ILLNESS, OR MAJOR SYSTEM DAMAGE (REQUIRES IMMEDIATE ACTION TO PREVENT A CAT I).

CATEGORY III: MARGINAL - MAY CAUSE MINOR INJURY, ILLNESS, OR SYSTEM DAMAGE (REQUIRES ACTION TO PREVENT A CAT II).

CATEGORY IV: NEGLIGIBLE - WILL NOT RESULT IN INJURY, ILLNESS, OR SYSTEM DAMAGE.

FIGURE 9a

MISHAP LIKELIHOOD

A: LIKELY TO OCCUR WITHIN A SHORT PERIOD OF TIME

B: PROBABLY WILL OCCUR IN TIME

C. MAY OCCUR IN TIME

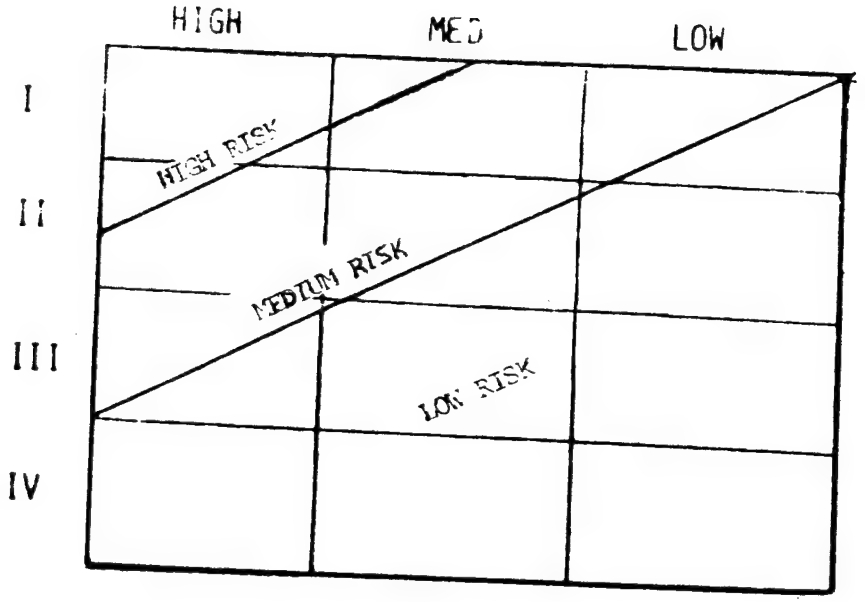
D: UNLIKELY TO OCCUR

FIGURE 9b

RISK LEVEL

SEVERITY	PROBABILITY			
	A	B	C	D
I	1	2	3	4
II	1	2	3	4
III	3	3	4	5
IV	5	5	6	6

FIGURE 9c



HAZARDOUS = CAT I OR II WITH HIGH PROBABILITY
(AFFTC/CC BRIEFED EACH FLIGHT)

MEDIUM = CAT I OR II WITH MODERATE PROBABILITY
OR CAT III WITH HIGH PROBABILITY
(6510TW/CC BRIEFED EACH FLIGHT)

FIGURE 10

flight.) The next area is Medium Risk. (Cat I or II with moderate probability of occurence or Cat III with the high probability of occurence.) These tests must be briefed to the wing commander prior to flight. Finally, those tests that fall in the lower right hand corner are considerd Low Risk and are managed by the squadron commander at or by the combined test force commander.

Another subjective method of quantifying risk is the use of the Real Hazard Index (RHI). Although similar to the risk assessment code, it does not use the matrix (see figures 11 and 12). The severity of hazard severity is defined in MIL STANDARD 882B, and each category is assigned a risk value of one through four, shown on the right hand side of the figure 11. Figure Y depicts word descriptors for the probability of occurrence of those hazards. Now the Real Hazard Index is nothing more than the product of those two numbers: ranging from a law of one to the maximum of 24. The SPO or the program manager will often make an arbitrary decision to correct any hazard with a real hazard index of greater than some preselected value, say 12, and ignore those below. Attached to these notes you will find a document called a Risk Management Guide for Air Force Operations published by the Directorate of Safety at Norton AFB. In this text you will also find another description of the real hazard index using different severity levels and an entirely different set of word descriptions. The Real Hazard Index can be used with many types of hazard severity definition or probability description.

Another method of quantifying risks was recently developed by two

HAZARD LEVELS

4 CATEGORY I: CATASTROPHIC - MAY CAUSE DEATH OR SYSTEM LOSS.

3 CATEGORY II: CRITICAL - MAY CAUSE SEVERE INJURY, ILLNESS, OR MAJOR SYSTEM DAMAGE (REQUIRES IMMEDIATE ACTION TO PREVENT A CAT I).

2 CATEGORY III: MARGINAL - MAY CAUSE MINOR INJURY, ILLNESS, OR SYSTEM DAMAGE (REQUIRES ACTION TO PREVENT A CAT II).

1 CATEGORY IV: NEGLIGIBLE - WILL NOT RESULT IN INJURY, ILLNESS, OR SYSTEM DAMAGE.

FIGURE 11

	DESCRIPTOR	UNIT USE	FLEET USE
6	FREQUENT	FREQUENTLY	CONTINUOUS
5	PROBABLE	WILL OCCUR SEVERAL TIMES IN LIFE OF UNIT	WILL OCCUR FREQUENTLY
4	OCCASIONAL	LIKELY TO OCCUR SOMETIME	WILL OCCUR SEVERAL TIMES
3	REMOTE	SO UNLIKELY YOU ASSUME WILL NOT OCCUR	UNLIKELY BUT POSSIBLE
2	IMPROBABLE	PROBABILITY CANNOT BE DISTINGUISED FROM 0	SO UNLIKELY YOU ASSUME WILL NOT OCCUR
1	IMPOSSIBLE	PHYSICALLY IMPOSSIBLE TO OCCUR	

gentlemen from the Navy: Mr Kenneth J. Graham, a research chemist at the Detonation Physics Division of the Naval Weapons Center at China Lake, and Dr Gilbert H. Kennedy, a distinguished professor from Chemical Engineering at the Naval Postgraduate School at Monterey, California. Together they conducted research on accident statistics and risk analysis and then published an article called a Practical Safety Analysis System for Hazards Control.

Their analysis is based on the following: risks are the product of the severity, the likelihood, and the exposure factor (Risk = Severity x likelihood x exposure). The severity, or consequence as they call it, is shown in figure 13. The consequence, ranging from 1 to 100 as they call it, is determined subjective by word description or may be determined empirically by the following equation: C = ($damage/100)0.4. The likelihood is also defined by a continuum from .1 to 10: from something that is virtually impossible to something that might well be expected. See figure 14. The exposure factors are based on the word descriptions shown in figure 15. A product of those three numbers yields a score used to subjectively evaluate the risk. See figure 16. This graduation of risk is more useful than the Real Hazard Index.

Practical use of this method might be as follows: For some hazards that have a very high risk (above 320) that point could be a point where you might consider grounding the fleet or grounding the airplane. It is a high risk with immediate correction required (160-320), one might opt for grounding the airplane within ten days pending some sort of an inspection.

	CONSEQUENCE	
100	CATASTROPHIC, MANY FATALITIES	$> \$10^7$
40	DISASTER, MULTIPLE FATALITIES	$\$10^6$-$10^7$
15	VERY SERIOUS, A FATALITY	$\$10^5$-$10^6$
7	SERIOUS, SERIOUS INJURY	$\$10^4$-$10^5$
3	IMPORTANT, DISABILITY	$\$10^3$-$10^4$
1	NOTICEABLE, FIRST AID MAYBE	$\$10^2$-$10^3$

$$C = \left(\frac{\text{DAMAGE}}{100}\right)^{0.4}$$

FIGURE 13

LIKELIHOOD

10	MIGHT WELL BE EXPECTED
6	QUITE POSSIBLE
3	UNUSUAL BUT POSSIBLE
1	ONLY REMOTELY POSSIBLE
0.5	CONCEIVABLE, BUT HIGHLY UNLIKELY
0.2	PRACTICALLY IMPOSSIBLE
0.1	VIRTUALLY IMPOSSIBLE

FIGURE 14

EXPOSURE FACTORS

10	CONTINUOUS
6	DAILY DURING WORKING HOURS
3	WEEKLY OR OCCASIONALLY
2	MONTHLY
1	A FEW TIMES PER YEAR
0.5	VERY RARE

FIGURE 15

RISK SCORE	
> 320	VERY HIGH RISK, CONSIDER DISCONTINUING
160-320	HI RISK, IMMEDIATE CORRECTION REQUIRED
70-160	SUBSTANTIAL RISK, CORRECTION REQUIRED
20-70	POSSIBLE RISK, ATTENTION NEEDED
< 20	SLIGHT RISK, ACCEPTABLE

FIGURE 16

If a correction is required (70-160) one might opt for a routine type TCTO; there is no great urgency but the situation should be corrected. If the risk score is 20 to 70, attention is needed, but that might be the type of action where only a Note or a Caution in the dash one is warranted to correct the action.

Further, these two gentlemen proposed a method to evaluate the cost effectiveness of any corrective action that might be proposed. In this analysis, the risk reduction effectiveness is the product of a risk reduction multiplier and risk score previously developed, divided by a cost divisor. The risk reduction multiplier is the percentage of the reduction of the hazard. For example, something that would reduce the hazard potential by 60% is assigned a risk reduction multiplier of .6; if it is 100% risk reduction, then the reduction value is 1.0.) The cost divisor is empirically derived cost from ($Cd = \sqrt[3]{\frac{\text{TOTAL COST}}{100}}$). Specifically, it is the cube root of a total cost divided by 100. The cost effectiveness is determined by the equation: cost effectiveness = $\frac{\text{RISK REDUCTION MULTIPLIER}}{\sqrt[3]{\frac{\text{COST}}{100}}} \times$. The degree of effectiveness of various systems can be evaluated in this manner. (See figure 17). Effectiveness scores greater than 20 indicate that the corrective device is very worth while; scores less than 10 indicate the fix is of doubtful merit.

The mathematics used in systems safety, are nothing more than probabilities and statistics. A short refresher in probabilities is in order. Consider the probability that during the flip of a coin it will be a head. This is obviously 50-50, assuming it cannot land on the edge. We

COST EFFECTIVENESS

M = RISK REDUCTION MULTIPLIER 60% REDUCTION = .6

100% REDUCTION = 1.0

C = COST DIVISOR = 3 $\frac{\text{TOTAL COST}}{100}$

EFFECTIVENESS = RISK SCORE X MX C

FIGURE 17

COST EFFECTIVENESS

20 HIGHLY WORTHWHILE

10-20 JUSTIFIED

10 OF DOUBTFUL MERIT

reach that conclusion, a priori, by simply deducing the possible ways it can land each flip divided by the total number of ways it can land. Similarly the probability of any given number on a die will appear is 1/6, only one number can come up although there are six possibilities.

Consider the probability of being able to roll five 6s in one roll and win a free drink at the bar. That is the chance of the first dice being a six, the second one being a six, the third one being a six and so on. The total probability that you can roll five 6s in one roll will of course be 1/6 times itself five times. (Probability = $(1/6)^5$). That means the first dice is a six and the second one is a six and the third one is a six, etc. When you use the verb "and" you are multiplying individual probabilities.

Consider another possibility: what is the probability of five sixes in one roll or five aces in one roll, in which case the bar will buy you and your friends a drink. The probability that you may roll five sixes in one roll or five ones in one roll are simply the two separate cases added together. Note the verb "or" means to add. That's the probability of five sixes in one plus the probability of five ones in one! Those are very important in using the "and" and "or" gates in the fault tree analysis which was discussed earlier. When you reach an "and" gate, the two probabilities are multiplied together; when it's an "or" gate it's the sum of all the probabilities going into that "or" gate.

Consider for a moment the popular Soviet party game called Russian Roulette. At first glance you will recognize the probability of becoming a fatality in a game of Russian Roulette, if you were to play only one time,

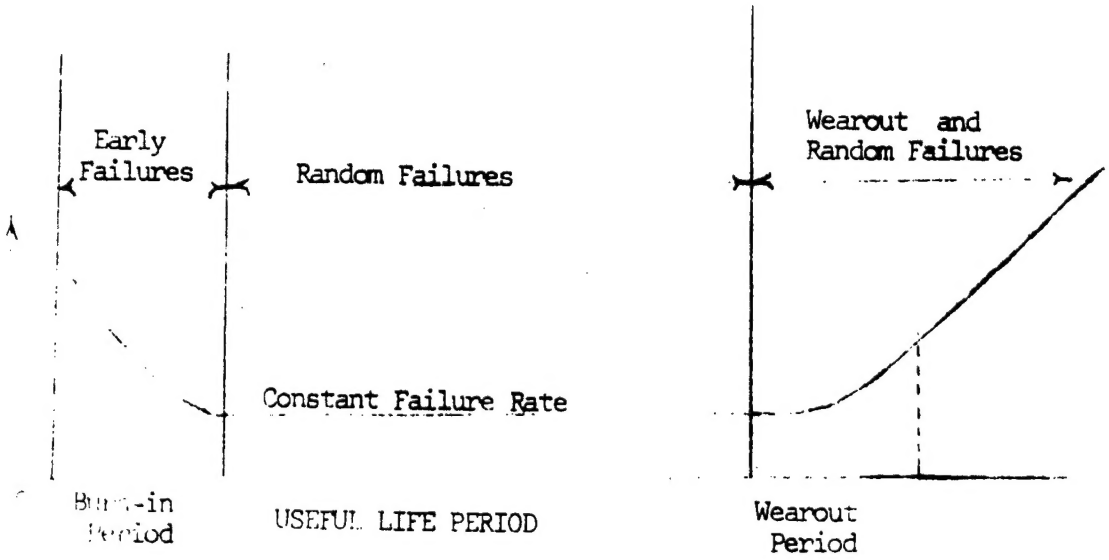
is obvious one-sixth: One chance out of six. But what are the odds that the bullet under the chamber is a dud or what is the probability the firing pin might fail? Considering the state of mind of one who would play Russian Roulette, what are the chances that he actually would hit himself when he pulled the trigger? You can see that actually the odds of death would be the product of all: (1/6 and probability of no dud and probabilty of no failure and probability, of not missing.)

How might you determine the various reliability rates? Determining the bullet reliabilities are probably rather easily obtained. You can locate the manufacturer who has a guaranteed a specified rate of reliability on his bullets, say no more than five out of a thousand would fail. The reliability is at least .995. Or perhaps he may have the acceptance test on that particular lot of ammunition where, out of a thousand rounds fired at random out of the lot only four failed; therefore, the reliability of that particular lot of ammunition could be considered .996. These are empirically derived reliability figures. Calculating the reliability of the revolver might be a little more difficult. Each manufacturer generally has an acceptance test which his product must pass before it is delivered to the market. Every gun is test fired. During the initial firings revolvers have a high failure rate, say perhaps 20 out of a thousand fail to fire the first time. The revolver that fails to fire is returned to the factory production division for refurbishment eg. to replace a broken spring, dent hammer, etc. whatever it was that caused the failure to fire. That revolver is again returned for acceptance test and on the second attempt to fire, generally it would fire. By the time each pistol is fired ten times the reliability rate

is very, very high, say maybe one out of a thousand would fail to fire. If a sample of, say ten or more revolvers, were tested to complete failure, or to wear out, you would see a curve that looks something like that shown in figure 18. As you near the service life of the revolver, the springs begin to break, the firing pins wear, etc., as the revolver wears out. This curve is called a "bathtub curve" because it's shaped somewhat like a bathtub, and it is used for predicting reliability of hardware. A word of caution: when you are doing flight test you are actually performing on the left hand side of the bathtub, so the failure rates generally are a lot higher than those of a proven system!

Now let's suppose for a moment that the reliability of the revolver and the bullets are of sufficiently high order, that you can consider the probabilty being killed in a round of Russian Roulette to be 1/6.

If six people were going to play the game, and after each player pulled the trigger, should he survive, he would spin the chamber and hand it to the next guy. If a player was fatally injured, the remaining players would reload and continue the game until all six had the opportunity to play. What is the probability that six can play and <u>someone</u> be killed in the game? That is the probability that <u>one</u> gets killed, plus the probability that <u>two</u> would be killed, plus the probability that <u>three</u> would get killed etc., up to the probability that all six were fatally injured. Since the sum of all individual probabilities must equal one, you could also solve that problem by subtracting the probability that none were killed from one or unity: $1 = P_0 + P_1 + P_2 + \ldots P_n$ $P_0 = 1 - P_0$. Now what is the probability that



BATHTUB CURVE

FIGURE 18

none are killed? Well that's the probability that a player would survive on any one round, and the next guy would survive, and the third guy would survive, etc. or, in other words, one minus 5/6 raised to the sixth power, and that turns out to be $(5/6)^6$ or .3349. The probability that someone is killed is then .6651.

Now if you were to ask an alternate question, namely what is the probability that exactly two were killed and exactly four survived, how would you solve that? How many combinations are there of two becoming killed and four surviving? The first two could be killed and the last four survive, the first and the last one killed, and the middle four survive, etc. The number of combinations are shown as follows: $\frac{6!}{(2!)(4!)} = 15.$ The general formula for determining probability is shown below: $\frac{n!}{x!(-x)!}$ $p^x q^{n-x}$ n is the total events in this case six players; x are the events of interest, i.e., 2 deaths; p is the probability that death will occur, in this event one sixth; q is the probability that death will not occur, in this event, five sixths. If you solve this you find the probability of exactly two killed and four survive is .16745.

Seldom do you have the opportunity to work with specifics such as described above. Generally you must consider a continuum of events, or continuum of probabilities. For that you use a general formula for empirical distribution called "a Poisson distribution." Here is the formula:

$$1 = e^{-\lambda t} + \frac{\lambda t e^{-\lambda t}}{1} + \frac{\lambda t e^{-\lambda t}}{1} + \frac{(\lambda t)^2 e^{-\lambda}}{2!} + \frac{(\lambda t)^n e^{-\lambda t}}{n!}$$

In the world of accident prevention you are interested in preventing the first accident. What is the probability of all possible number of accidents occurring: one, two, three,

Etc? As before, solve by subtracting probability of no accidents occurring from 1. $P_{a24} = 1 - e^{-\lambda/t} = 1 - P_o$. This is Murphy's Law; it shows that if lambda is anything other than zero, (if there's a way for sombody to screw it up) then if there is enough time, (somebody will in fact screw it up) and the probability Pany approaches unity (accident will occur).

Lambda is the failure rate or the inverse of the mean time between failure (MTBF). If so you're runing a test rig to determine mean time between failure, you can extract the failure rate directly.

Systems Safety, as applied here at the Flight Test Center, is more appropriately called Test Program Safety, since we are here more interested in the actual conduct of the test than we are of the physical design of the hardware. You, as test engineer or the flight test pilot, prepare a test plan. While you are preparing a test plan, you must consider the hazards involved. Using the AFSC Form 5028 described earlier in the text, list all the hazards, their causes, their effects, and controls you might employ to prevent the occurrence of that hazard.

When your test plan has been written, it will be reviewed by engineers for technical content. This review is primarily technical although safety matters may be considered. Once that review has been accomplished then you will meet a system Safety Review Board (SRB). You, your supervisors, and the System Safety Division will mutually determine the composition of the board. The board will usually consist of operation and engineering representatives plus others as required: The operations representative is preferably current in the type aircraft under test and is in a supervisory

or independent position. The engineering representatives are supervisors or experts from the disciplines involved: i.e., propulsion, aerodynamic, flutter, etc. Occasionally there will be a maintenance personnel represented if there is significant maintenance involvement. Many test, need representation the Fire Department or the hospital if lasers or toxic materials are used or are part of the test.

When the deliberations are complete a risk assessment is determined, (hazardous test, medium risk or low risk as shown by the matrix discussed earlier). The complete AFSC Form Form 5028 is signed by board members and supervisors as shown on the front side of the Form 5028. After the commanders have seen these documents, the test plan and Form 5028 is briefed to the Commander, Vice Commander, and the Test Wing Commander regardless of the risk level.